

日 本 国 特 許 庁
JAPAN PATENT OFFICE

JC879 U.S. PTO
09/911235



別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office

出 願 年 月 日

Date of Application:

2000年 8月 3日

出 願 番 号

Application Number:

特願2000-235605

出 願 人

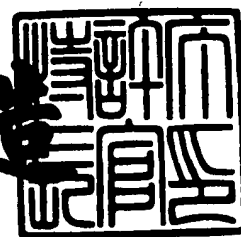
Applicant(s):

ソニー株式会社

2001年 5月30日

特許庁長官
Commissioner,
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3044755

【書類名】 特許願

【整理番号】 0000540801

【提出日】 平成12年 8月 3日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 15/177

【発明者】

【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内

【氏名】 末吉 正弘

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代表者】 出井 伸之

【連絡先】 知的財産部 03-5448-2137

【手数料の表示】

【予納台帳番号】 005094

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 OS上のセキュアなタスク間通信方法

【特許請求の範囲】

【請求項1】 OS（オペレーティング・システム）上で実行されるタスク自身の鍵からタスクと上記OSとの相互認証が成功したセキュリティ有りのレベルと相互認証を行っていないセキュリティ無しのレベルとに分類して、各タスク自身のセキュリティの有無とタスクと上記OSとの相互認証用鍵とを上記OS側でテーブル形式で管理する第1ステップと、

上記OS側で管理されている上記セキュリティ有りのレベルのタスクのブロックごとと、上記セキュリティ無しのレベルのタスクのブロックごとにセキュア・メモリ管理機構によりセキュア・メモリ・ブロックと、ノン・セキュア・メモリ・ブロックに分けて読み書きする第2ステップと、

上記セキュリティ有りのレベルのタスクのメール送信用タスク上にメール送信用バッファを用意するとともに、上記セキュリティ有りのレベルのタスクのメール受信用タスク上にメール受信用バッファを用意して、上記OS内にメール内容を格納するメモリ領域と管理情報を格納するメモリ領域とを用意する第3ステップと、

上記メール送信用タスクでセキュリティ・レベル以外にメールID、送信タスク側で割り当てられたメール本体へのアドレスを指定し、OS側で上記メール送信用タスクのセキュリティ・レベルと送信用関数のセキュリティ・レベルを基にどのメモリ・ブロックを使用するかを判断して、メール送信用タスクがセキュリティ有りで、かつ送信時レベルがセキュリティ有りの場合のみ、上記セキュリティ・メモリ・ブロックに管理情報を書き込み、メール送信内容をメールID、管理情報のアドレス値、メール本体のアドレス値を鍵として暗号化した内容を書き込む第4ステップと、

上記メール受信用タスク側で、セキュリティ・レベル以外に上記メール送信用タスクと同一のメールID、メール受信用タスク側で割り当てられたメール本体へのアドレスを指定し、上記OSによりメール受信用タスクのセキュリティ・レベルと受信関数のセキュリティ・レベルを基にどのセキュリティ・メモリ・プロ

ックを使用するかを判断して、メール受信用タスクがセキュリティ有りであり、かつ受信時レベルがセキュリティ有りの場合のみ、上記セキュリティ・メモリ・ブロックで管理されているメール受信用タスク宛ての該当受信メールを検索して、受信内容が存在するバッファの内容をメールID、管理情報のアドレス値、メール本体のアドレス値を鍵として復号化した内容を上記メール受信用タスク上のバッファにコピーする第5ステップと、

を含むことを特徴とするOS上のセキュアなタスク間通信方法。

【請求項2】 上記認証は、タスクごとに持つ鍵を上記セキュアOS側で管理している鍵と同一であるか、否かの照合により行うことを特徴とする請求項1記載のOS上のセキュアなタスク間通信方法。

【請求項3】 上記セキュア・メモリ管理機構は、上記メモリ・ブロックをブロックごとにセキュリティ・レベルに応じたアクセス許可、不許可の設定が可能なハードウェアであることを特徴とする請求項1記載のOS上のセキュアなタスク間通信方法。

【請求項4】 上記セキュア・メモリ管理機構は、セキュリティ・レベル無しのメール送信用タスクあるいはメール受信用タスクに対してセキュリティ有りのメモリ・ブロックへの読み書きはできないことを特徴とする請求項1記載のOS上のセキュアなタスク間通信方法。

【請求項5】 上記セキュアOSは、タスクごとのセキュリティ・レベルの管理と上記セキュア・メモリ管理機構を介した上記メモリ・ブロックの管理を一元的に行うことを特徴とする請求項1記載のOS上のセキュアなタスク間通信方法。

【請求項6】 上記管理情報は、メール・サイズとメール本体のポインタとで構成されることを特徴とする請求項1記載のOS上のセキュアなタスク間通信方法。

【請求項7】 上記メール送信用タスクの内容は、実態を上記セキュア・メモリ・ブロック中に有るセキュア・メモリ・プールから確保することを特徴とする請求項1記載のOS上のセキュアなタスク間通信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、OSとOS上で実行されるタスクの構成において、タスク自身のセキュリティ・レベルと、タスク側で送信、受信時に指定されるセキュリティ用モードの有無をOS側で判定し、セキュリティ有りの場合はアクセス制限されたメモリ領域から通信用作業領域を獲得し、送信内容を暗号化するようにしたOS上のセキュアなタスク間通信方法に関する。

【0002】

【従来技術】

通常のOS上のタスク間通信においては、送受信されるデータ内容を隠蔽および秘匿するための記憶が存在しないために、第三者が制作したソフトウェア・モジュールにより読み書きすることが可能である。

そこで、OSを介して伝送されるデータの隠蔽を実現するため、送信側タスクが設定するセキュリティの有無に応じたタスク間通信（たとえば、メール）を実現可能な機構を発明するに至った。

たとえば、特開平08-106441号公報では、マイクロアーキテクチャ方式のOSを前提としてセキュリティ・レベルを持つプロセス間通信方式が記載されている。

【0003】

【発明が解決しようとする課題】

しかし、この公報の場合には、OS外部に認証局に相当するトラステイド・サーバが必要であるという課題がある。

【0004】

この発明は、上記従来課題を解決するためになされたもので、認証局をOSの外に持たない代わりに、OS自身が送信内容本体のハードウェアによるアクセス制限と送信内容の暗号化を実現することにより、組み込み用途に配慮することができ、セキュリティ・レベルに応じたタスク処理が混在した環境で、鍵操作や暗号化、復号化を行うタスクにはセキュリティ有りのレベルを与え、セキュリティをもつタスク間通信の秘匿性を高めることができ、タスクとタスク間通信のサ

ービス起動時にセキュリティ・レベルが個別に指定可能であり、両者の組み合わせによりタスク間通信の内容本体のアクセス制限が実現できるOS上のセキュアなタスク間通信方法を提供することを目的とする。

【0005】

【課題を解決するための手段】

上記目的を達成するために、この発明のOS上のセキュアなタスク間通信方法は、OS（オペレーティングシステム）上で実行されるタスク自身の鍵からタスクと上記OSとの相互認証が成功したセキュリティ有りのレベルと相互認証を行っていないセキュリティ無しのレベルとに分類して、各タスク自身のセキュリティの有無とタスクと上記OSとの相互認証用鍵とを上記OS側でテーブル形式で管理する第1ステップと、上記OS側で管理されている上記セキュリティ有りのレベルのタスクのブロックごとと、上記セキュリティ無しのレベルのタスクのブロックごとにセキュア・メモリ管理機構によりセキュア・メモリ・ブロックと、ノン・セキュア・メモリ・ブロックに分けて読み書きする第2ステップと、上記セキュリティ有りのレベルのタスクのメール送信用タスク上にメール送信用バッファを用意するとともに、上記セキュリティ有りのレベルのタスクのメール受信用タスク上にメール受信用バッファを用意して、上記OS内にメール内容を格納するメモリ領域と管理情報を格納するメモリ領域とを用意する第3ステップと、上記メール送信用タスクでセキュリティ・レベル以外にメールID、送信タスク側で割り当てられたメール本体へのアドレスを指定し、OS側で上記メール送信用タスクのセキュリティ・レベルと送信用関数のセキュリティ・レベルを基にどのメモリブロックを使用するかを判断して、メール送信用タスクがセキュリティ有りで、かつ送信時レベルがセキュリティ有りの場合のみ、上記セキュリティ・メモリ・ブロックに管理情報を書き込み、メール送信内容をメールID、管理情報のアドレス値、メール本体のアドレス値を鍵として暗号化した内容を書き込む第4ステップと、上記メール受信用タスク側で、セキュリティ・レベル以外に上記メール送信用タスクと同一のメールID、メール受信用タスク側で割り当てられたメール本体へのアドレスを指定し、上記OSによりメール受信用タスクのセキュリティ・レベルと受信関数のセキュリティ・レベルを基にどのセキュリテ

ィ・メモリ・ブロックを使用するかを判断して、メール受信用タスクがセキュリティ有りであり、かつ受信時レベルがセキュリティ有りの場合のみ、上記セキュリティメモリ・ブロックで管理されているメール受信用タスク宛ての該当受信メールを検索して、受信内容が存在するバッファの内容をメールID、管理情報のアドレス値、メール本体のアドレス値を鍵として復号化した内容を上記メール受信用タスク上のバッファにコピーする第5ステップとを含むことを特徴とする。

そのため、メール送信用タスクと、メール受信用タスク自身のセキュリティ・レベルと、タスク側で送信時、受信時に指定するセキュリティ用モード有りとセキュアOS側で判断すると、セキュアOS側が転送用データの実態とタスク間通信路を確立するための管理用データをセキュア・メモリ・ブロックに割り当て、セキュアOS側で転送用データを鍵により暗号化し、メール受信用タスクのデータを復号化する。

また、タスクとタスク間通信のサービス起動時にセキュリティ・レベルが個別に指定可能となる。

【0006】

【発明の実施の形態】

次に、この発明によるOS上のセキュアなタスク間通信方法の実施の形態について図面に基づき説明する。

具体的な実施の形態の説明に先立ち、まず、この発明の特徴を概説する。この発明は、OSとOS上で実行されるタスクの構成において、タスク自身のセキュリティ・レベルとタスク側で送信、受信時に指定するセキュリティ用モードの有無をOS側で判断し、セキュリティ・レベルの異なるタスク間通信路を実現する。

また、セキュリティ用モードが有りと判断された場合には、OSが転送用データの実態およびタスク間通信路を確立するための管理用データをアクセス制限されたメモリに割り当てる。

一方、セキュリティ用モードが無いと判断された場合には、両者のデータをアクセス制限の無い一般のメモリに割り当てる。

さらに、タスク側でセキュリティ用モードが有りと判断された場合には、OS

が転送用データの実態を鍵により暗号化する。

【0007】

次に、このような特徴を有するこの発明による第1実施の形態を詳細に説明する。

説明の都合上、図2から説明する。

この図2は、この第1実施の形態に適用されるセキュアOS1上のタスク2、3のセキュリティ・レベルを説明するための説明図である。

この第1実施の形態では、セキュリティ有り、無しの2つのレベルを想定している。

セキュアOS1側とタスクとによる相互認証が成功したタスク2、3（図2では、タスク2をタスクA、タスクBとして示している。）をセキュリティ有りのレベルとし、また、この相互認証を行っていないか、相互認証の失敗、または未処理のタスク3（図2では、タスクCとして示している）をセキュリティ無しのレベルとする。

【0008】

このセキュアOS1側とタスク2、3とによる相互認証の方法は、たとえば、タスク2、3ごとに鍵を持ち、セキュアOS1側で管理している鍵とタスク2、3の持っている鍵とが一致した場合にセキュリティ有りのレベルとし、また、両者の鍵が一致しない場合には、セキュリティ無しのレベルとし、図2では、上述のように、タスク3がセキュリティ無しのレベルとしている場合を示している。

これらのタスク2、3自身のセキュリティの有無と相互認識用鍵をセキュアOS1側がテーブル4の形式で管理する。

すなわち、セキュリティ有りのレベルのタスク2、セキュリティ無しのレベルのタスク3、これらのタスク2、3の持っている鍵の各データはこのテーブル4の形式でセキュアOS1側の内部で保持している。

【0009】

次に、セキュアOS1側のメモリ・ブロック管理について図1を参照して説明する。この図1における読み書き可能なRAMなどによるメモリ・ブロック5は、ノン・セキュア・メモリ・ブロック5aと、セキュア・メモリ・ブロック5b

とに2分されている。

ノン・セキュア・メモリ・ブロック5aには、NO. 1、3、……、n-1のように奇数番目のアドレスにタスク3のようなセキュリティ無しのレベルがブロックで書き込まれる。

また、セキュア・メモリ・ブロック5bには、NO. 2、4、……、nのように偶数番目のアドレスにタスク2のようなセキュリティ有りのレベルがブロックで書き込まれる。

【0010】

すなわち、メモリ・ブロック5は、タスクをブロックごとにセキュリティ・レベルの設定が可能なMMU6（メモリ管理機構：以下、SMMUという）により読み書きする。

このSMMU6は、読み書きする側のセキュリティ・レベル、すなわち、セキュアOS1側のセキュリティ・レベル（さらに換言すれば、サービスを要求したタスクのセキュリティ・レベル）とノン・セキュア・メモリ・ブロック5aに書き込まれているセキュリティ・レベルと、セキュア・メモリ・ブロック5bに書き込まれているセキュリティ・レベルとを比較して、読み書きする側のセキュリティ・レベルが低い場合には、セキュリティ・アクセス違反例外が発生し、セキュア・メモリ・ブロック5b、ノン・セキュア・メモリ・ブロック5aへ読み書きが不可能になる。

【0011】

言い換えれば、サービスを要求したタスクよりも、セキュリティ・レベルが高いセキュア・メモリ・ブロック5b、ノン・セキュア・メモリ・ブロック5aへのアクセスがセキュリティ・アクセス違反例外が発生してセキュア・メモリ・ブロック5b、ノン・セキュア・メモリ・ブロック5aへ読み書きが不可能になる。

このSMMU6は、メモリ5をセキュア・メモリ・ブロック5b、ノン・セキュア・メモリ・ブロック5aごとに、セキュリティ・レベルに応じたアクセス許可、不許可の設定が可能なハードウェアである。

たとえば、このSMMU6は、セキュリティ・レベル無しの状態で、セキュリ

ティ有りのセキュア・メモリ・ブロック 5 b への読み書きはできないものとする。

【0012】

セキュア・メモリ・ブロック 5 b、ノン・セキュア・メモリ・ブロック 5 a に対するセキュリティ・レベルの設定は、セキュア OS 1 の初期時に SMMU 6 により、テーブル 7 に示すように行う。

このテーブル 7 は、セキュア・メモリ・ブロック 5 b、ノン・セキュア・メモリ・ブロック 5 a のアドレスに対するセキュリティ有無と、鍵の各データが対応している。

また、セキュア OS 1 がタスクごとのセキュリティ・レベルの管理と、SMMU 6 を介したセキュア・メモリ・ブロック 5 b、ノン・セキュア・メモリ・ブロック 5 a の管理を一元的に行う。

【0013】

次に、セキュリティ有りタスク間通信を行う場合について図 1 を参照して説明する。このタスク間通信はメールであり、上記タスク 2 について、図 1 では、メール送信用タスク 2 として説明する。また、タスク 3 について、図 1 では、メール受信用タスク 3 として説明する。

メール送信用タスク 2 上にメール送信用バッファ 8（サーバ用バッファ）を用意するとともに、メール受信用タスク 3 上にメール受信用バッファ 9 を用意する。

【0014】

また、セキュア OS 1 内にメール内容を格納するメモリ領域をセキュア・メモリプール 10 a, 10 b の形式で用意する。

管理情報を格納するメモリ領域（上記ノン・セキュア・メモリ・ブロック 5 a、セキュア・メモリ・ブロック 5 b に相当）をノン・セキュア・メモリ・キュー・リスト 11 a、セキュア・メモリ・キュー・リスト 11 b の形式で用意する。

図 4 は管理情報 12 の構成を示すものであり、管理情報 12 は、メール・サイズ 12 a とメール本体へのポインタ 12 b で構成されている。

【0015】

ノン・セキュア・メモリ・キュー・リスト 1 1 a、セキュア・メモリ・キュー・リスト 1 1 b と、セキュア・メモリ・プール 1 0 a、1 0 b は、上記セキュア・メモリ・ブロック 5 b、ノン・セキュア・メモリ・ブロック 5 a に個別に用意される。

【0016】

次に、メール送信用タスク 2 と受信用タスク 3 はセキュア OS 1 側と相互認証が正常に終了し、これらのメール送信用タスク 2 と受信用タスク 3 自身のセキュリティ・レベルが有りに設定されている場合に、メール送信用タスク 2 でタスク間通信用関数（たとえば、メール）をセキュリティ・レベル有り付きで送信する場合の処理の流れを図 5 のフローチャートに沿って説明する。

まず、スタートして、メール送信用タスク 2 側では、セキュリティ・レベル以外に、メール ID、メール送信用タスク側で割り当てられたメール本体へのアドレスを指定する。

メール送信用タスク 2 がセキュリティ・オン・レベルでメール送信サービスを要求し（ステップ S 1）、メール送信用タスク 2 が送信されて、セキュア OS 1 側でこのメール送信用タスク 2 の要求を受け取ると（サービスでもよい）（ステップ S 2）、セキュア OS 1 側では、受信したメール送信用タスク 2 がセキュリティ・レベルとメール・サービスであるかをチェックする（ステップ S 3）。

【0017】

次いで、セキュア OS 1 側では、この受信されたメール送信用タスク 2 とメール・サービスがセキュリティ・レベルであるか、どうかを判断して、さらに、送信用関数〔図 8（a）にメール送信用関数として示されている〕のセキュリティ・レベルを基に受信されたメール送信用タスク 2 に対して、セキュア・メモリ・ブロック 5 b、あるいはノン・セキュア・メモリ・ブロック 5 a のどちらのメモリ・ブロックを使用するかを判断する（ステップ S 4）。

この判断の結果、この受信されたメール送信用タスク 2 がセキュリティ有りのレベルで、かつ送信時のレベルがセキュリティ有りの場合にのみ、ステップ S 5 の処理に進み、セキュア OS 1 側では、SMMU 6 によりセキュア・メモリ・ブロック 5 b で管理されているセキュア・メモリ・キュー・リスト 1 1 b の中の管

理情報とメール本体を検索する。

【0018】

次いで、この検索した管理情報とメール本体から1要素のメール本体に管理情報を書き込む。

この場合、メール送信用タスク2の内容は、セキュリティ有りのセキュア・メモリ・ブロック5bに格納されているセキュア・メモリ・プール10bから確保する。

次に、図6に示すメール本体の暗号化フローチャートに示すように、セキュア・メモリ・プール10bから確保したメール送信内容のメール本体に、SMMU6によりメールIDを書き込み（ステップS11）、管理情報のアドレス値を書き込み（ステップS12）、メール本体のアドレス値を書き込んで、これらの値を鍵としてメール送信内容を暗号化し（ステップS13）、その暗号化したメール送信内容を、図5のステップS6で上記バッファ8（サーバ用バッファ）からセキュア・メモリ・キュー・リスト11bで管理されるバッファ13へコピーする。

次いで、セキュアOS1側では、管理情報を更新して（ステップS7）、上記一連のメール送信処理を終了する。

【0019】

また、上記ステップS4の処理において、セキュアOS1側では、受信されたメール送信用タスク2のサービスのセキュリティと、さらに、タスク間通信用関数のセキュリティ・レベルを基に受信されたメール送信用タスク2に対して、セキュア・メモリ・ブロック5b、あるいはノン・セキュア・メモリ・ブロック5aのどちらのメモリブロックを使用するかを判断した結果、受信されたメール送信用タスク2がセキュリティ有りのレベルで、かつ送信時のレベルがセキュリティ有りでない場合には、セキュアOS1側では、SMMU6によりノン・セキュア・メモリ・ブロック5aから管理情報とメール本体を検索する（ステップS8）。

【0020】

次いで、セキュアOS1側は、メール本体にメール送信用タスク2の内容を書

き込み、バッファ 8 に書き込んで（ステップ S 9）、上記ステップ S 7 の処理を行う。

【0021】

次に、メール受信用タスク 3 でタスク間通信用関数（たとえば、メール）をセキュリティ・レベル有り付で受信する処理の流れについて図 7 のフローチャートに沿って説明する。

メール受信用タスク 3 側では、セキュリティ・レベル以外に、メール ID、メール受信用タスク 3 側で割り当てられたメール本体へのアドレスを指定する。メール ID は、送信側と同一の値を指定する。

次いで、メール受信用タスク 3 は、セキュリティ・オン・レベルのメール受信サービスを要求し（ステップ S 21）、メール受信用タスク 3 側でメール受信用タスク 3 のメール・サービスを行うと、セキュア OS 1 側はメール受信用タスク 3 のサービスを受信する（ステップ S 22）。

【0022】

次いで、セキュア OS 1 側はこの受信したメール受信用タスク 3 とメール・サービスが、セキュリティ有りのレベルであるか、否かのチェックを行い（ステップ S 23）、そのチェックの結果、セキュリティ有りのレベルであると、次に、セキュア OS 1 側はメール受信用タスク 3 とサービスがともに、セキュリティ有りのレベルであるか、否かの判定を行い（ステップ S 24）、その判定の結果、両方ともにセキュリティ有りのレベルであると判断すると、セキュア OS 1 側はメール受信用タスク 3 のセキュリティ・レベルと、受信用関数 {図 8（b）にメール受信関数として示されている} のセキュリティ・レベルとを基にどのセキュア・メモリ・ブロックを使用するかを判断を行う。

【0023】

この判断の結果、メール受信用タスク 3 がセキュリティ有りのレベルで、かつ受信時のレベルがセキュリティ有りのレベルの場合にのみ、セキュア・メモリ・ブロック 5 b で管理されているメール・キュー・リスト内のメール受信用タスク 3 宛ての該当メールを検索し（ステップ S 25）、受信内容が存在するバッファを見付ける。

このバッファ内容をメールID、管理情報のアドレス値、メール本体アドレス値を鍵として復号化した内容をメール受信用タスク3上のバッファ9へコピーする（ステップS26）。

次いで、セキュアOS1側は、メール本体と管理情報とを戻して（ステップS27）、一連の受信処理を終了する。

【0024】

また、上記ステップS24の処理において、セキュアOS1側はメール受信用タスク3とサービスがともに、セキュリティ・レベルであるか、否かの判定を行い（ステップS24）、その判定の結果がともに、セキュリティ・レベルでない場合であると、判断すれば、セキュアOS1側はノン・セキュア・メモリ・ブロック5aにおける管理情報を検索する（ステップS28）。

次いで、セキュアOS1側は、メール受信用タスク3上に用意したバッファ9にメール本体をコピーした後に（ステップS29）、上記ステップS27の処理を行う。

【0025】

【発明の効果】

以上のように、この発明によれば、メール送信用タスクと、メール受信用タスク自身のセキュリティ・レベルと、タスク側で送信時、受信時に指定するセキュリティ用モード有りとセキュアOS側で判断すると、セキュアOS側が転送用データの実態とタスク間通信路を確立するための管理用データをセキュア・メモリ・ブロックに割り当て、セキュアOS側で転送用データを鍵により暗号化し、メール受信用タスクのデータを復号化するようにしたので、鍵操作や暗号化・復号化を行うタスクには、セキュリティ有りのレベルを与えるような、セキュリティ・レベルに応じたタスク処理が混在した環境で、タスク間通信の内容がアクセス制限される機構において、セキュリティを持つタスク間通信の秘匿性を高めることができる。

また、タスクとタスク間通信のサービス起動時にセキュリティ・レベルが個別に指定可能であり、指定されたセキュリティ・レベル2つを組み合わせることによりタスク間通信の内容本体のアクセス制限を実現することができる。

【図面の簡単な説明】

【図 1】

この発明によるOS上のセキュアなタスク間通信方法の第1実施の形態に適用されるタスク間通信を行う場合の構成要素の説明図である。

【図 2】

この発明によるOS上のセキュアなタスク間通信方法の第1実施の形態に適用されるセキュアOS上のタスク・セキュリティ・レベルを説明するための説明図である。

【図 3】

この発明によるOS上のセキュアなタスク間通信方法の第1実施の形態に適用されるセキュアOS側のセキュア・メモリ・ブロックの管理を説明するための説明図である。

【図 4】

この発明によるOS上のセキュアなタスク間通信方法の第1実施の形態に適用されるメール管理情報の構成説明図である。

【図 5】

この発明によるOS上のセキュアなタスク間通信方法の第1実施の形態に適用されるメール送信処理を説明するためのフローチャートである。

【図 6】

この発明によるOS上のセキュアなタスク間通信方法の第1実施の形態に適用されるメール本体の暗号化フローを示すフローチャートである。

【図 7】

この発明によるOS上のセキュアなタスク間通信方法の第1実施の形態に適用されるメール受信処理フローを示すフローチャートである。

【図 8】

この発明によるOS上のセキュアなタスク間通信方法の第1実施の形態に適用されるメール送受信関数例を示すフローチャートである。

【符号の説明】

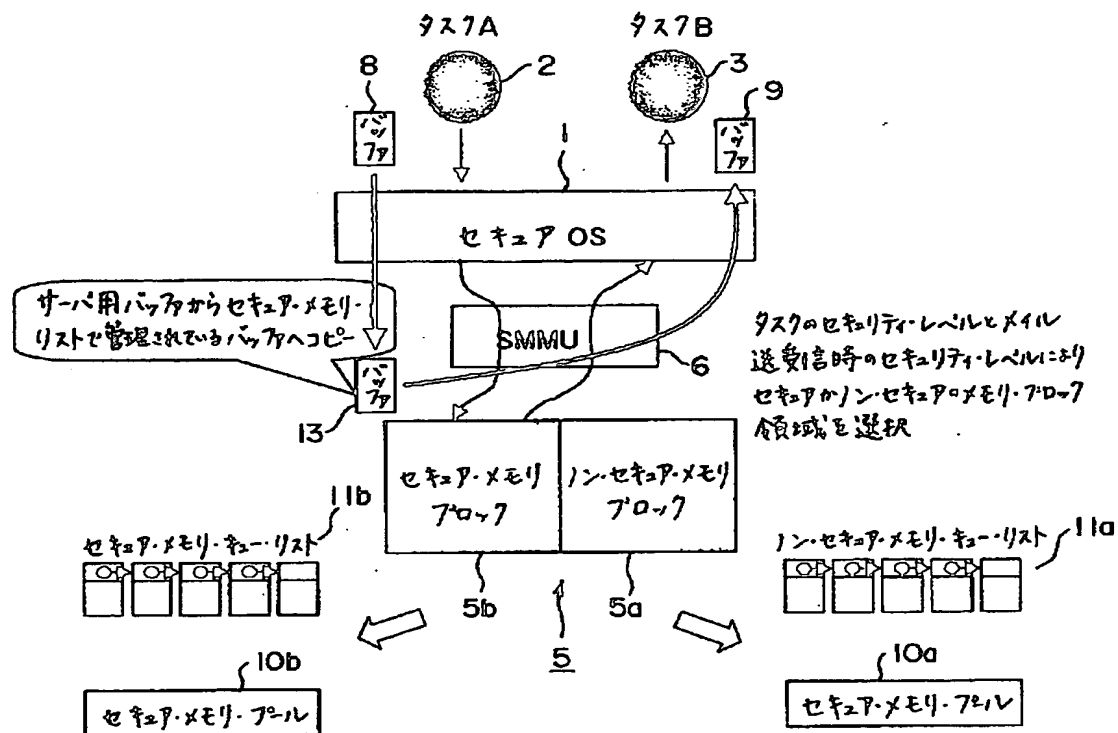
1 ……セキュアOS、 2 ……メール送信用タスク、 3 ……メール受信用タスク

、 4 , 7 …… テーブル、 5 …… メモリ・ブロック、 5 a …… セキュア・メモリ・
ブロック、 5 b …… ノン・セキュア・メモリ・ブロック、 6 …… SMMU (メモ
管理機構)、 8 , 9 …… バッファ、 1 0 a , 1 0 b …… セキュア・メモリ・プー
ル、 1 1 a …… ノン・セキュア・メモリ・キュー・リスト、 1 1 b …… セキュア
・メモリ・キュー・リスト、 1 2 …… 管理情報、 1 2 a …… メール・サイズ、 1
2 b …… ポインタ。

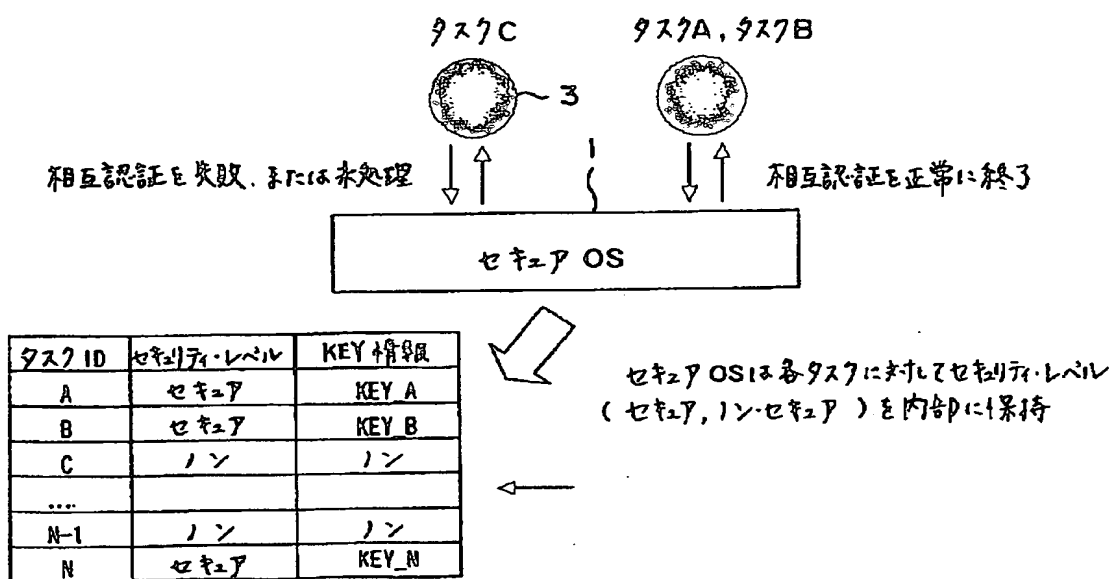
【書類名】

図面

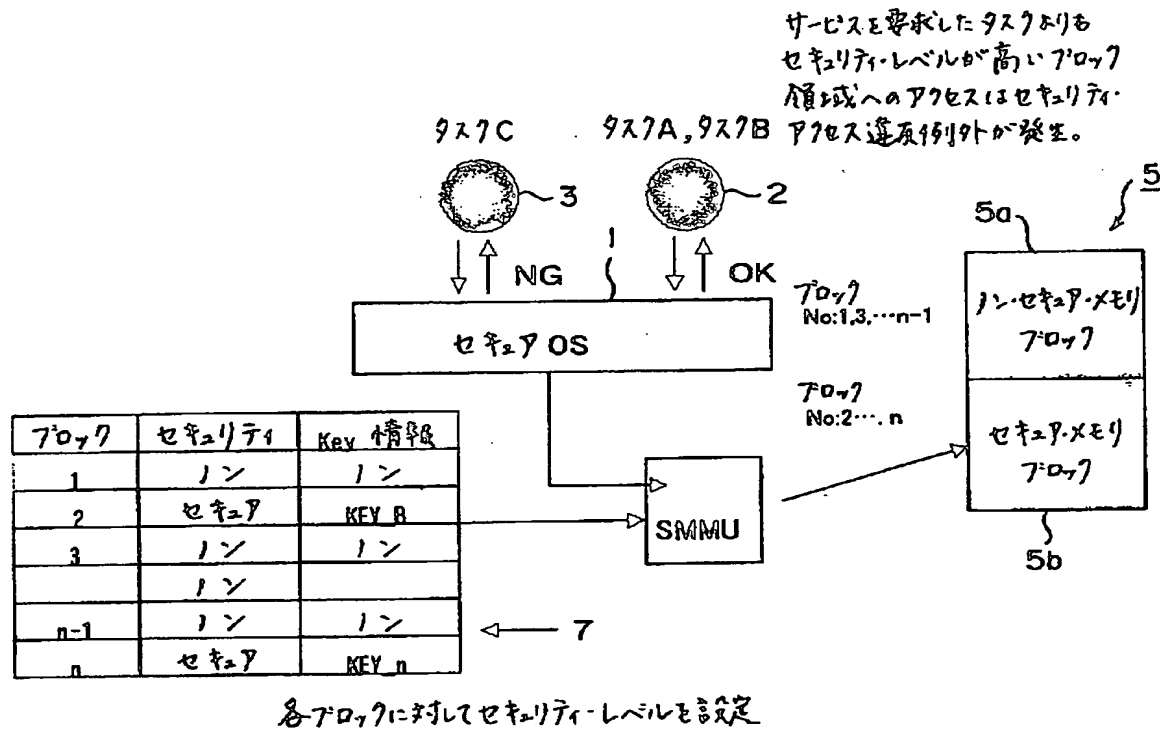
【図 1】



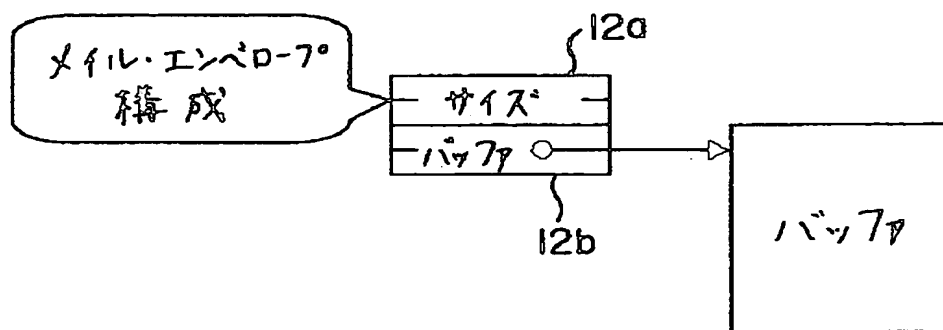
【図 2】



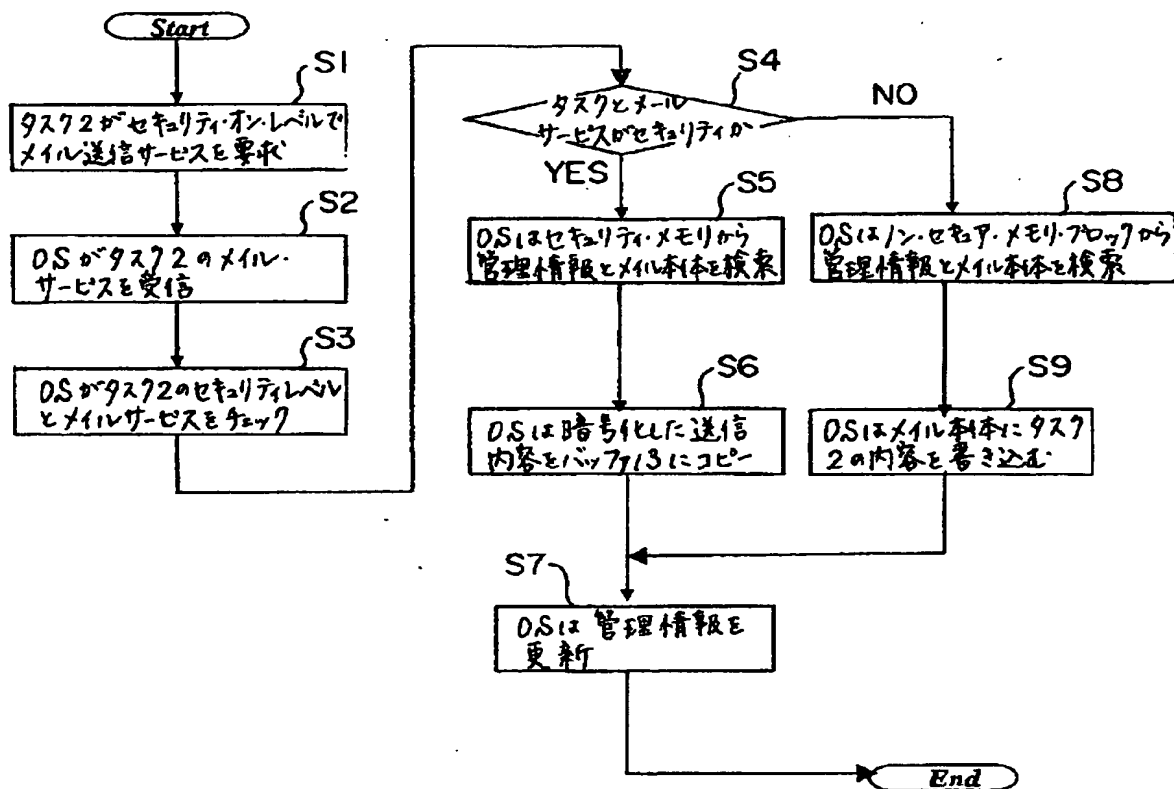
【図3】



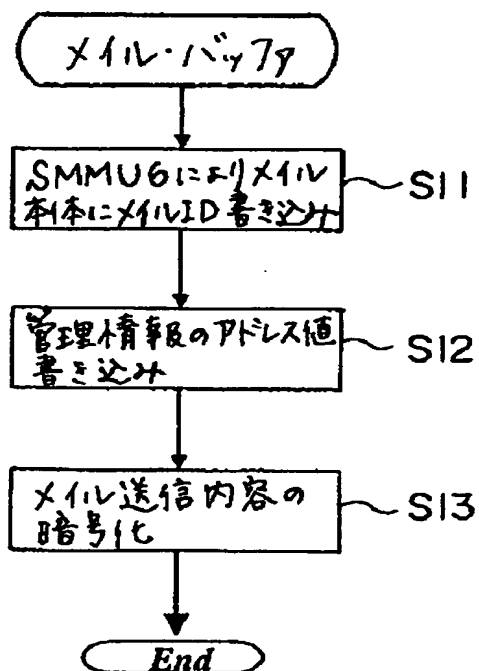
【図4】



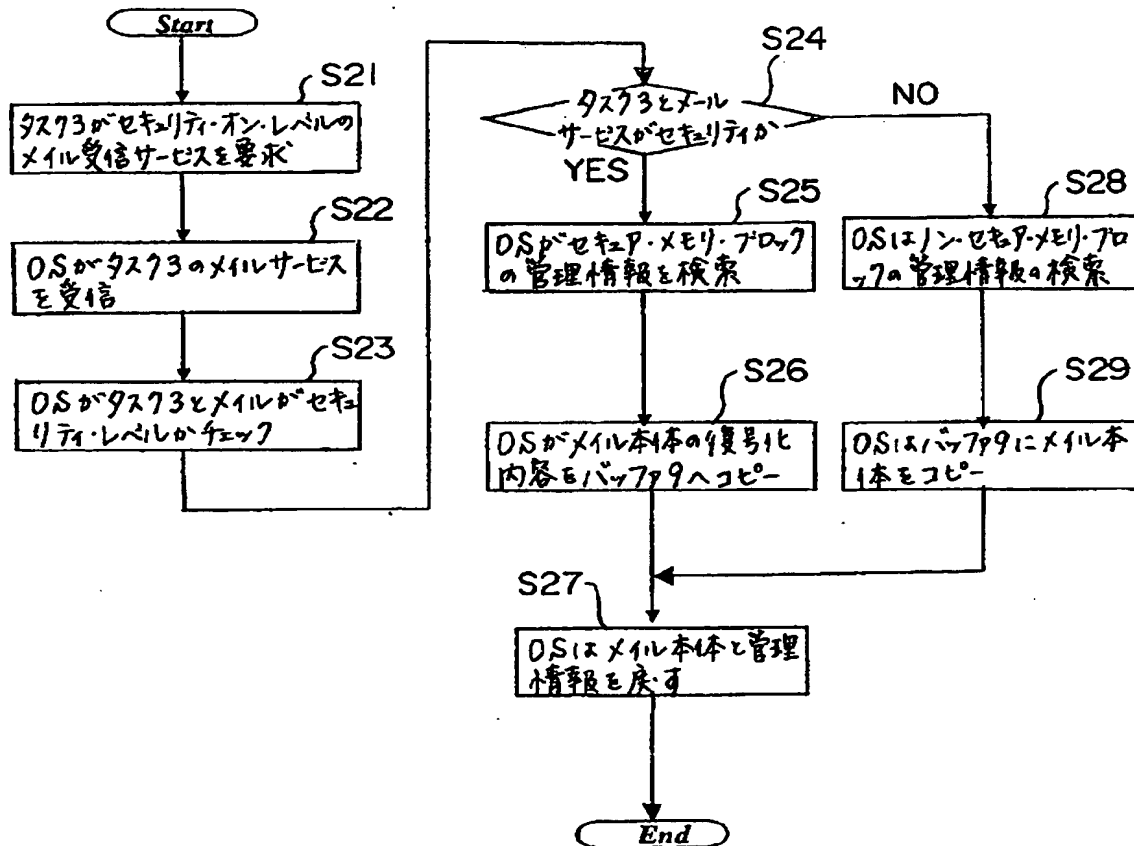
【図 5】



【図 6】



【図 7】



【図 8】

メール送信

(a) SendMail(int MailBoxNumber, MailBuf *buf, int SecurityLevel)

メール受信

(b) RecvMail(int MailBoxNumber, MailBuf *buf, int SecurityLevel)

【書類名】 要約書

【要約】

【課題】 セキュリティを持つタスク間通信の秘匿性を高めるOS上のセキュアなタスク間通信方法を提供すること。

【解決手段】 メール送信用タスク2側でメールID、メール本体へのアドレスを指定し、セキュアOS1で、メール送信用タスク2のセキュリティ・レベルと送信用関数のセキュリティ・レベルを基に、セキュア・メモリ・キュー・リスト11b中の1要素に管理情報を書き込み、メール送信内容をメールID、管理情報のアドレス値、メール本体のアドレス値を鍵として暗号化した内容をバッファ8に書き込む。

セキュアOS1はメール受信用タスク3のセキュリティ・レベルと受信用関数のセキュリティ・レベルを基に受信内容の存在するバッファの内容をメールID、管理情報のアドレス値、メール本体のアドレス値を鍵として復号化してメール受信用タスク3上のバッファ9にコピーする。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 2 1 8 5]

1. 変更年月日	1 9 9 0 年 8 月 3 0 日
[変更理由]	新規登録
住 所	東京都品川区北品川 6 丁目 7 番 3 5 号
氏 名	ソニー株式会社